The undersigned Assistant U.S. Attorney has reviewed the entire search warrant package and approves it

Digitally signed by SEAN WELSH
Date: 2024.08.16 15:42:08 -04'00'

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF VIRGINIA
HARRISONBURG DIVISION

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH GETTR ACCOUNT JOEMADARATS1 THAT IS STORED AT PREMISES CONTROLLED BY GETTR USA, INC.	Case No. 5:24-mj-00064

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Steven W. Duke, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with GETTR user account joemadarats1 ("TARGET ACCOUNT") that is stored at premises owned, maintained, controlled, or operated by GETTR USA, INC., an electronic communications and social media service provider headquartered at 3 Columbus Circle, New York, New York.

2. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require GETTR to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

3. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been since January 2009. As such, I am a law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510(7) and am empowered by law to conduct investigations and to make arrests for offenses enumerated in 18 U.S.C. § 2516. I am currently assigned to the Winchester Resident Agency of the FBI Richmond Field Office.

4. As a Special Agent of the FBI, I have investigated violations of federal law and have gained experience and knowledge through investigations and training, and from discussions with law enforcement officers with experiences and training in investigating violations of federal law. I have been involved in the use of the following investigative techniques: interviewing victims, witnesses, and subjects; conducting physical surveillance; consensual monitoring; analyzing records associated with social media accounts, IP addresses, phone numbers, financial records, email accounts, and telephone tolls; and assisting with Title III and consensual wiretap investigations. Through my work, I have also talked to other investigators with experience investigating these types of offenses and learned about the types of evidence typically gathered from the execution of search warrants, including searches of social media and email accounts. As a law enforcement officer, I am authorized to execute warrants issued under authority of the United States.

5. The facts in this affidavit come from a variety of sources, including: my personal observations and participation in this investigation; my training and experience; information obtained from other agents, task force officers, and witnesses; information obtained through records and databases; and other sources, which I believe to be reliable. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. This affidavit also reflects my current

understanding of facts relating to this investigation, but my understanding may change in the future as the investigation proceeds. Similarly, where information contained in reports and other documents or records are referenced herein, such information is also described in sum and substance and in relevant part only. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

6. Unless otherwise stated, the conclusions and beliefs I express in this affidavit are based on my training, experience, and knowledge of the investigation, and reasonable inferences I have drawn from my training, experience, and knowledge of the investigation.

7. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Section 115 (Threating Federal Officials), Title 18, United States Code, Section 871 (Threatening the President of the United States and Successors to the Presidency), Title 18, United States Code, Section 875(c) (Threatening Interstate Communications), and Title 18, United States Code, Section 879 (Threatening Former Presidents and Certain Other Persons) have been committed by FRANK CARILLO. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

8. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

A. GETTR THREATS

9. On July 27, 2024, at 2:47 p.m. EST, Maricopa County, Arizona, Recorder's office notified FBI Phoenix of potential threats to the Maricopa County Recorder, "Victim-1" made by the GETTR[1] TARGET ACCOUNT. Specifically, the TARGET ACCOUNT posted "someone need to remove this asshole permanently someone needs to kill this fuck." FBI Phoenix conducted further open-source research on the TARGET ACCOUNT and identified further threatening statements directed at several public officials.

10. FBI Phoenix submitted legal process to GETTR and received responsive records on July 29, 2024. The responsive records from GETTR revealed approximately 4,359 posts/replies made by the TARGET ACCOUNT targeting various public officials including but not limited to: President Joseph Biden, Vice President Kamala Harris, FBI Director Christopher Wray, Victim-1, and many other public officials.

11. Specifically, President Biden was referenced 197 times by the TARGET ACCOUNT and included violent comments, some examples of which are below:

11/27/2023 – "JOE BIDEN AND THIS ADMIN MUST DIE"

03/11/2024 – "WE NEED TO ASSASSINATE SCUM LIKE JOE BIDEN AN HIS ADMIN"

03/11/2024 – "JOE BIDEN MUST DIE WITH HIS ADMIN"

05/18/2024 – "SUPPLY ME THE MONEY AND JOE BIDEN IS HISTORY"

05/19/2024 – "BIDEN WILL ALWAYS BE A DUMBASS WHO DOES NOT CARE FOR THIS COUNTRY HE MUST BE ASSASSINATED"

---

[1] GETTR is a social media platform and micro blogging website. User interface and features have been described as very similar to "X", formerly known as Twitter.

07/15/2024 – "It's the dance Joe Biden bum f****** Biden scumbag Biden f****** mumbling stuttering Biden you're a waste of life and soon your life will be wasted"

12. Vice President Kamala Harris was mentioned 19 times by the TARGET ACCOUNT. Some examples of the violent comments aimed at Vice President Harris are below:

07/27/2024 – "Listen to me crappler Harris also known as cunt Harris you don't have a snowballs chance in hell which is exactly where you're going and soon I will cut your eyes out of your FUCKING head while you're alive bitch and I will make sure you suffer a slow agonizing death you piece of shit"

07/27/2024 – "Kamala Harris needs to be put on fire alive I will do it personally if no one else does it I want her to suffer a slow agonizing death"

07/27/2024 – "Harris is going to regret ever trying to become president because if that ever happened I will personally pluck out her eyes with a pair of pliers but first I will shoot and kill everyone that gets in my way that is a f****** promise"

07/27/2024 – "Just for being a Democrat you're going to die crap La Harris that's a f****** promise I'm going to find you and your f****** family and I'm going to kill you all you f****** waste of life I can't wait to rip your eyes out of your f****** head with a pair of eyes you piece of s*** and nothing but scum of the Earth and you're going to die like it"'

07/27/2024 – "Crapler Harris is laying thieving piece of garbage like the rest of this administration they all need to die and they will soon"

13. The TARGET ACCOUNT mentioned FBI Director Christopher Wray 8 times. Some of the violent comments directed at FBI Director Wray are below:

04/12/2024 – "WRAY SHOULD DIE LIKE HE LIVES WITH HIS FINGERS UP HIS ASS"

07/27/2024 – "No Wray should be hung by his neck until he dangles to death"

07/27/2024 – "WRay is a liar and a scumbag he's also bought and sold he must pay for his actions with his life and his family's life they almost died severely"

14. Former President Barack Obama was mentioned 48 times by the TARGET ACCOUNT. Some examples of the violent comments directed toward former President Obama are below:

> 11/24/2023 – "THAT'S OBAMA FAULT AND HE SHOULD PAY WITH HIS LIFE SOON"
>
> 12/03/2023 – "NOW MAKE ALL OF THE OBAMAS PAY WITH THEIR LIVES WITH ALL THE OTHER SCUM WHO STARTED THIS"
>
> 07/27/2024 – "Soon Barack Obama and his whole family will be dead the people will kill them we will torture them to death and then we will hang them just like they belong hung in the nearest tree so everyone can see the scum that they are a naked walk over to them and carve their initials in them that is their whole family I don't give a f*** who it is but the whole family is going to die we will hunt you down and we will torture to you to death"
>
> 07/27/2024 – "I think he's taking a big chance with the CIA they work for f****** scumbag Obama he's going to die no matter what whether you getting office or not he will die and he will suffer dying Obama and his f**** disgusting vile wife boyfriend whatever the f*** you want to call him they will die the whole family will die that is my promise we the people have spoken"
>
> 07/27/2024 – "Soon Barack Obama and his whole family will be dead the people will kill them we will torture them to death and then we will hang them just like they belong hung in the nearest tree so everyone can see the scum that they are a naked walk over to them and carve their initials in them that is their whole family I don't give a f*** who it is but the whole family is going to die we will hunt you down and we will torture to you to death"

15. Other public officials referenced in threatening statements include Senators Chuck Schumer and Mitch McConnell, former Secretary of State Hillary Clinton, former President Bill Clinton, and Congresswoman Nancy Pelosi, and others.

16. On February 22, 2024, the TARGET ACCOUNT posted on GETTR "I HAVE MY AR-15 LOCKED AND LOADED".

B. IDENTIFICATION OF FRANK CARILLO

17. Through legal process, FBI Phoenix obtained the subscriber information from GETTR USA, Inc., for the TARGET ACCOUNT. Based on the responsive information from GETTR with the date range of June 15, 2023, through July 28, 2024, the TARGET ACCOUNT was created on June 15, 2023, and is associated with email address joemadarats588@gmail.com.

i. GETTR Location Information

18. On or about July 27, 2024, the TARGET ACCOUNT posted 46 comments to the GETTR service using two different Internet Protocol (IP) addresses. Posts submitted to GETTR by the TARGET ACCOUNT between 7:36 AM - 8:07 AM used IP address 172.58.253.113, and between 9:17 AM - 7:35 PM used IP address 204.111.228.117.

19. Reviews of open-source records indicate that the service provider for IP address 172.58.253.113 is T-Mobile USA, Inc, and the service provider for 204.111.228.117 is GLO Fiber, which is a subsidiary of Shentel. GLO Fiber/Shentel was unable to provide subscriber information associated with the IP address without a port number, which GETTR did not provide to law enforcement. GETTR has advised law enforcement that it does not capture port numbers.

ii. Google Location Information

20. FBI Phoenix submitted legal process to Google, LLC, for subscriber and device information connected to joemadarats588@gmail.com. Analysis of subscriber information associated with joemadarats588@gmail.com revealed that the Google account was created on or about January 18, 2020. The name associated with joemadarats588@gmail.com is "Joe Madarats" and included a recovery email of bobungots61@gmail.com and recovery phone number of 1-610-762-5261. IP addresses associated with login activity for joemadarats588@gmail.com revealed that the account used IP address 204.111.228.117 18 times on or about July 26, 2024 - July 29,

2024. In addition, on July 29, 2024, joemadarats588@gmail.com used IP address 2607:fb91:dc4:aa75:2458:deff:fe94:c84f one time. Open-source records indicate that the service provider for IP address 2607:fb91:dc4:aa75:2458:deff:fe94:c84f is T-Mobile USA, Inc.

21. Google, LLC, also provided the device IMEI number 356125201089732, which belongs to an Android phone and is associated with joemadarats588@gmail.com. The device account identifiers also provide additional email accounts connecting to the device which includes email address fcarillo@hotmail.com, among others.

22. In addition, Google, LLC, provided logins to the account associated with joemadarats588@gmail.com, which showed logins to the account on July 26-29, 2024, were made with IP address 204.111.228.117. This IP address is the same IP address that is seen with the threatening GETTR posts that were posted by the TARGET ACCOUNT on July 27, 2024.

23. Analysis of the Google Location History records associated with joemadarats588@gmail.com revealed 220 records with approximate device locations for the moto g G5 device for July 27, 2024, between 4:09 AM - 10:03 PM. During this time period, all 220 records indicated that the moto g G5 device was in the immediate vicinity of the Preston Place Apartment and Townhomes located north of Airport Road near Winchester, Virginia. This area includes the residence of FRANK CARILLO, which is located at "Address-1"[2] in Winchester, Virginia. The entirety of the 220 records includes a display radius of 6 meters to 123 meters. Analysis of records with a display radius of 20 meters or less indicated that there are 71 records with approximate locations in the immediate vicinity of the townhomes on the west side of the same block as Address-1 (odd house numbers), which also includes the residence of CARILLO.

[2] Address-1 is known to law enforcement but redacted here for privacy.

iii. Android Device Information

24. Analysis of Google Android Device Configuration Service Data records indicated that the mobile device used to login to joemadarats588@gmail.com was a Motorola moto g 5G uniquely identified with international mobile equipment identity (IMEI) 356125201089732. The moto g 5G was first used with Google's services on or about July 13, 2024, and continued through July 29, 2024. Google indicated that the subscriber identity module (SIM) card associated with the phone were encoded with a mobile country code (MCC) of 310 and mobile network code (MNC) of 240 and 260. A MCC of 310 indicates that the service provider associated with the SIM is in the United States, and both MNCs of 240 and 260 indicate that the mobile network operator is T-Mobile USA, Inc. The last data connection indicated on the Google records indicate that, at the time the Google records were obtained, the mobile device connected from IP address 2607:fb91:dc4:aa75:2458:deff:fe94:c84f. This IP address is the same IP address used to login to joemadarats588@gmail.com on July 29, 2024, and service is provided by T-Mobile USA, Inc.

25. The Google Android Device Configuration Service Data also identified 6 additional email accounts that were associated with the moto g 5G mobile device. Two of the associated email addresses include bobungots61@gmail.com (recovery email for joemadarats588@gmai.com) and fcarillo@hotmail.com.

C. SEARCH WARRANT AND USE OF TARGET ACCOUNT

26. A federal search warrant was executed at Address-1, Winchester, Virginia, on August 2, 2024. At the time the warrant was executed, CARILLO and another individual ("Witness-1") were the only two individuals present at the residence.

i. Carillo's Statements

27. During his initial contact with law enforcement, CARILLO asked why this was happening, and Special Agent Nicholas Olson, FBI, indicated it was related to something posted online. A short time later, CARILLO, seemingly talking to himself, stated, "…for a comment. This is ridiculous, for a comment. I guess I'm gonna need a lawyer."

28. Additionally, CARILLO stated to another law enforcement officer, FBI Task Force Officer Zachary Hawkins, if it was "about the online stuff. I posted it." When CARILLO overhead law enforcement personnel discussing firearms in the residence, he indicated he had a 9mm handgun and an AR-15, which he had purchased in February.

29. Among other items, federal agents seized an RF-15 rifle[3] and a 9 mm handgun from inside the residence. According to Witness-1, those particular firearms belonged to CARILLO. Witness-1 believed CARILLO purchased the handgun in 2023 and the rifle in 2024. Law enforcement also recovered more than 2,000 rounds of ammunition for the firearms, which included more than 1,000 rounds of ammunition for the AR-15.

30. Following his request for an attorney, CARILLO stated, "This is all over a comment, huh?"

31. Following his arrest, CARILLO asked, "Is [Witness-1] being arrested?" When Special Agent Steven W. Duke, FBI, replied, "I don't know," CARILLO stated, "[Witness-1] didn't do anything. I made the comments."

[3] This is a specific brand of an AR-15 rifle.

ii. Witness-1's Statements

32. Witness-1 was interviewed by law enforcement. According to Witness-1, Witness-1 and CARILLO have resided in the townhouse for almost a year. During that time, no one else has lived in the residence.

33. Witness-1 advised law enforcement personnel at the scene that CARILLO utilized cellular telephone number 610-762-5261, which was the same number listed as the recovery phone number for joemadarats588@gmail.com.

34. Witness-1 identified aliases of CARILLO as "Joe Madrats" and "Bob Ugots." Witness-1 learned about these aliases from CARILLO. Witness-1 believed "Joe Madrats" was associated with an email address.

35. Witness-1 consented to a search of Witness-1's cell phone. Three photos taken in May 2024 were discovered on Witness-1's cell phone. The photos depicted the screen of another cell phone displaying email addresses and passwords. Witness-1 indicated the photos depicted CARILLO's cell phone displaying CARILLO's email addresses and passwords. The photos were taken to capture his passwords prior to getting a new cell phone. The photos displayed the following email addresses: joemadarats588@gmail.com, bsdmdmatter@gmail.com, cc0903571@gmail.com, bobungots61@gmail.com, and fcarillo@hotmail.com. The email addresses joemadarats588@gmail.com and bobungots61@gmail.com sounded familiar to Witness-1.

iii. Additional GETTR Information

36. Because the TARGET ACCOUNT was used to threaten violence against public officials, it is reasonable to assume that the TARGET ACCOUNT contains additional information

regarding the threats, as well as statements, plans, and other evidence concerning taking action on said threats.

37. A preservation request was served to GETTR for the TARGET ACCOUNT on July 28, 2024.

BACKGROUND CONCERNING GETTR[4]

38. GETTR USA, Inc., owns and operates GETTR, a social media platform that can be accessed at https://gettr.com and/or the GETTR mobile application ("app"). GETTR describes its service as an all-in-one social utility compatible with mobile and web platforms in every corner of the globe. Some features included with a GETTR account include traditional micro-blogging, livestreaming, in-app editing and filtering of images, in-app video editing, direct messaging, and the ability to post videos and images.

39. GETTR users can sign up for an account by using existing social media accounts such as Google, Apple, Facebook, X (formerly Twitter), and Amazon, or via a phone number or email address.

40. According to the GETTR privacy policy, GETTR has processed various categories of personal information from subscribers, including identifiers such as names, phone numbers, email addresses, unique personal identifiers, online identifiers, IP addresses, email addresses, and account names; commercial information such as records of personal property, products or services purchased, obtained, or considered, or other purchasing or consumer

---

[4] The information in this section is based on information published by GETTR on its website, including, but not limited to, the following documents and webpages: https://about.gettr.com ("About GETTR"), https://gettr.com/privacy ("GETTR Privacy Policy"), and https://gettr.com/landing ("GETTR overview").

histories or tendencies; internet or other electronic network activity information such as browsing history, search history, information on a consumer's interaction with a website, application logs, device data and registration, and social media account information or advertisement; geolocation data; and sensitive personal information (if the subscriber chooses to provide it) such as precise geolocation, account log-in, in combination with any required security or access code, password, or credentials allowing access to an account, personal information that reveals a consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership, and contents of mail, email, and text messages.

41. In my training and experience, evidence of who was using a social media account and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. For example, IP addresses associated with each GETTR login that resulted in a threatening post from the TARGET ACCOUNT could be used to positively identify the user of the TARGET ACCOUNT for each post; and any additional information available such as statements, videos, and direct messages could provide valuable information on actions to be taken to carry out the threats.

42. Based on my training and experience, direct messages, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. Thus, stored communications and files connected to a GETTR account may provide direct evidence of the offenses under

investigation and can also lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

43. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (*e.g.*, information indicating a plan to commit a crime), or consciousness of guilt (*e.g.*, deleting account information in an effort to conceal evidence from law enforcement).

44. Other information connected to the use of an account may lead to the discovery of additional evidence. For example, accounts are often assigned or associated with additional identifiers such as account numbers, advertising IDs, cookies, and third-party platform subscriber identities. This information may help establish attribution, identify and link criminal activity across platforms, and reveal additional sources of evidence.

CONCLUSION

45. Based on the forgoing, I believe that there is probable cause to believe that evidence to show that CARILLO has violated Title 18, United States Code, Section 115 (Threating Federal Officials), Title 18, United States Code, Section 871 (Threatening the President of the United States and Successors to the Presidency), Title 18, United States Code, Section 875(c) (Threatening Interstate Communications), and Title 18, United States Code, Section 879 (Threatening Former Presidents and Certain Other Persons) will be found in the TARGET ACCOUNT.

46. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on GETTR. Because the warrant will be served on GETTR, who will

then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

47. Based on the forgoing, I request that the Court issue the proposed search warrant.

OATH

I declare under penalty of perjury that the foregoing is true and correct.

Respectfully submitted,

s/Steven W. Duke
Steven W. Duke, Special Agent
Federal Bureau of Investigation

Received by reliable electronic means and sworn and attested to by telephone on this 19th day of August 2024.

JOEL C. HOPPE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with GETTR account joemadarats1 (the "Account") that is stored at premises owned, maintained, controlled, or operated by GETTR USA, INC., an electronic communications and social media service provider headquartered at 3 Columbus Circle, New York, New York.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by GETTR USA, Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of GETTR USA, Inc., regardless of whether such information is located within or outside of the United States, and including any communications, records, files, logs, or information that has been deleted but is still available to GETTR USA, Inc., or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on July 28, 2024, GETTR USA, Inc., is required to disclose to the government for each account or identifier listed in Attachment A:

A. The following information about the customers or subscribers of the Account, from the date the Account was created to the present, unless specified otherwise below:

1. Identity and contact information (past and current), including full name, e-mail address, physical address, date of birth, phone number, gender, and other personal identifiers;

2. All usernames (past and current) and the date and time each username was active, all associated accounts (including those linked by machine cookie, IP address, email address, or any other account or device identifier), and all records or other information about connections with third-party websites and mobile apps (whether active, expired, or removed);

3. Length of service (including start date), types of services utilized, purchases, and means and sources of payment (including any credit card or bank account number) and billing records, including for any paid services;

4. Devices used to login to or access the account, including all device identifiers, attributes, user agent strings, and information about networks and connections, cookies, operating systems, and apps and web browsers;

5. All advertising information, including any related IDs and ad activity;

6. Internet Protocol ("IP") addresses used to create, login, and use the account, including associated dates, times, and port numbers;

7. Privacy and account settings, including change history; and

8. Communications between GETTR USA, Inc., and any person regarding the account, including contacts with support services and records of actions taken;

B. All content, records, and other information relating to communications sent from or received by the Account from June 15, 2023, to August 2, 2024, including but not limited to:

1. The content of all posts created, drafted, favorited/liked, bookmarked, or reposted by the Account, and all associated multimedia, metadata, and logs;

2. The content of all direct messages sent from, received by, stored in draft form in, or otherwise associated with the Account, including all attachments, multimedia, header information, metadata, and logs;

C. All other content, records, and other information relating to all other interactions between the Account and other GETTR users from June 15, 2023, to August 2, 2024, including but not limited to:

1. All users the Account has followed, unfollowed, muted, unmuted, blocked, or unblocked, and all users who have followed, unfollowed, muted, unmuted, blocked, or unblocked the Account;

2. Lists of GETTR users who have favorited/liked, bookmarked, or reposted posts by the account, as well as all posts that include the username associated with the account (i.e., "mentions" or "replies");

3. All information about Communities of which the Account is a member, administrator, or moderator; including all posts created, drafted, favorited/liked, bookmarked, or reposted by the Account;

4. All contacts and related sync information; and

5. All associated logs and metadata;

D. All other content, records, and other information relating to the use of the Account, including but not limited to:

1. All data and information associated with the profile page, including photographs, "bios," and profile backgrounds and themes;

2. All multimedia uploaded to, or otherwise associated with, the Account;

3. All records of searches performed by the Account from June 15, 2023 to August 2, 2024.

4. All location information, from June 15, 2023, to August 2, 2024

GETTR USA, Inc., is hereby ordered to disclose the above information to the government within **14 days** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and/or instrumentalities of violations of Title 18, United States Code, Section 115 (Threating Federal Officials), Title 18, United States Code, Section 871 (Threatening the President of the United States and Successors to the Presidency), Title 18, United States Code, Section 875(c) (Threatening Interstate Communications), and Title 18, United States Code, Section 879 (Threatening Former Presidents and Certain Other Persons), those violations involving CARILLO occurring after June 15, 2023, including, for each Account or identifier listed on Attachment A, information pertaining to the following matters:

a. Records and information relating to threats of violence directed at government officials;
b. Records and information relating to Interstate communications related to threats of violence related to government officials;
c. Records and information relating to steps planned or taken regarding threats of violence;
d. Records and information relating to access of the GETTR platform, Facebook, and other social media platforms;
e. Records and information relating to the acquisition of firearms, the planned acquisition of firearms, and the use or trade of any firearms;
f. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to e-mail messages, chat logs and electronic messages, and other digital data files) pertaining to the communication related to target offenses;

g. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider;

h. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage;

i. Any and all digital records, diaries, notes, and any other records that contain information pertaining to defendant's past travel, including but not limited to international travel completed within the last year;

j. Evidence indicating how and when the Account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the account owner;

k. Evidence indicating the Account owner's state of mind as it relates to the crime under investigation;

l. The identity of the person(s) who created or used the Account, including records that help reveal the whereabouts of such person(s).

m. Any documents, communications, or financial records related to the acquisition or attempted acquisition of firearms, ammunition, and related equipment.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.